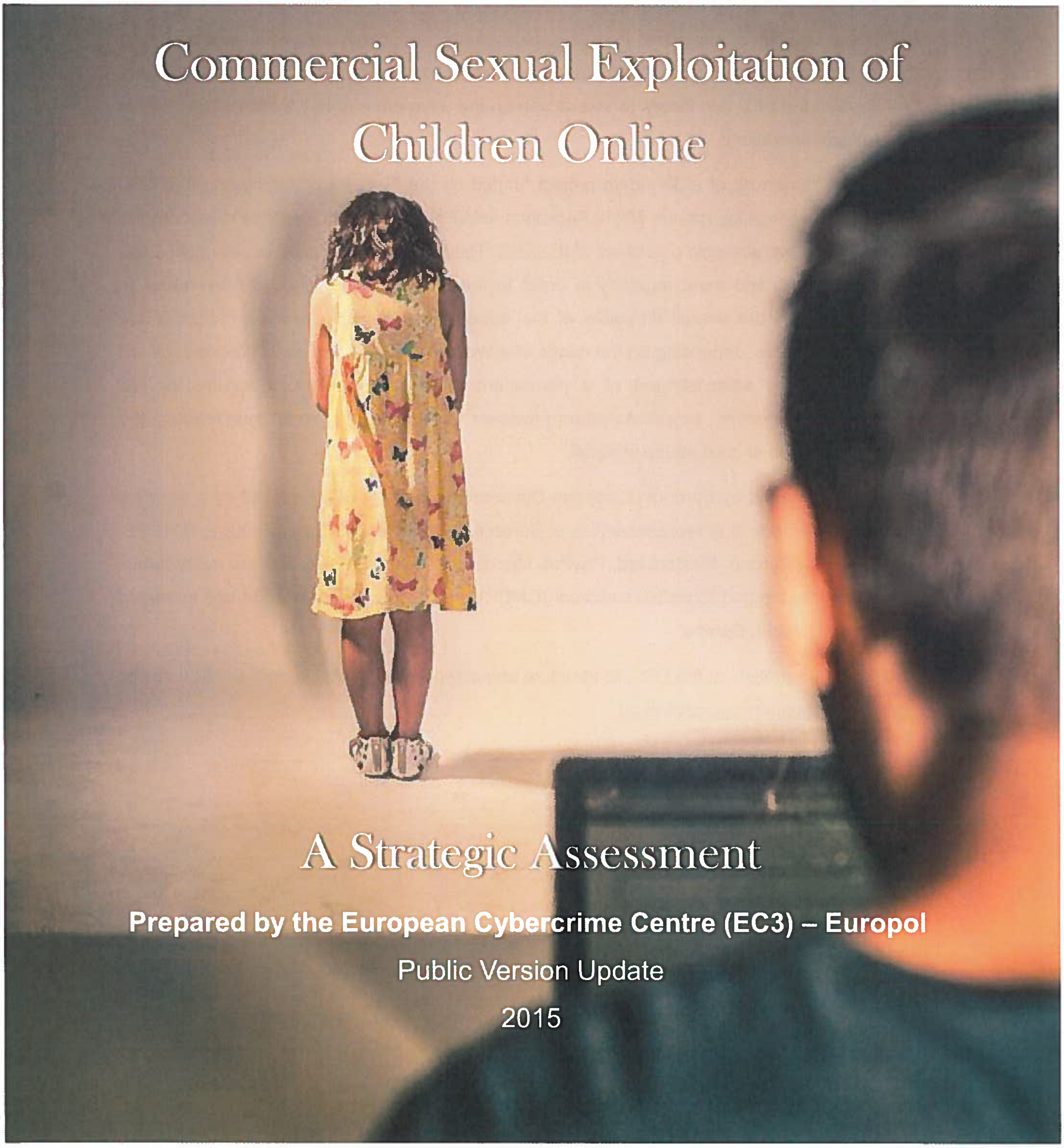
EUROPEAN FINANCIAL COALITION

against Commercial Sexual Exploitation of Children Online

Commercial Sexual Exploitation of Children Online



A Strategic Assessment

Prepared by the European Cybercrime Centre (EC3) – Europol

Public Version Update

2015

EC3 EUROPOL · Missing Children Europe · INHOPE · International Centre · VISA · MasterCard Worldwide · PayPal · Google · Microsoft · CEPOL · EUROJUST

This project has been funded with the support of the European Commission. This publication reflects the views only of the author. The European Commission cannot be held responsible for any use which may be made of the information contained therein.

The European Financial Coalition against Commercial Sexual Exploitation of Children Online (EFC) is a coalition of key actors from law enforcement, the private sector and civil society in Europe with the common goal of fighting the commercial sexual exploitation of children online. Members of the EFC join forces to take action on the payment and ICT systems used to run these illegal operations.

Within the framework of a 36-month project funded by the European Commission, the EFC focuses on five working groups (Work Packages or WPs). Each Work Package is responsible for one of the five strategic objectives of the EFC. The WPs are composed of both public and private partners, and meet regularly in order to implement their respective deliverables in accordance with the overall timetable of the three-year project. Relevant participants are identified over time, depending on the needs of a Work Package. The five working groups will contribute to the establishment of a permanent platform and resource centre for law enforcement authorities, payment system providers and ISPs engaged in counteracting the online distribution of child abuse material.

The EFC is chaired by Europol (European Cybercrime Centre – EC3) and led by a Steering Committee composed of representatives of Europol-EC3, Missing Children Europe, INHOPE, Eurojust, Visa Europe, MasterCard, PayPal, Microsoft, Google, CEPOL and the International Centre for Missing and Exploited Children (ICMEC). Its secretariat is hosted at and managed by Missing Children Europe.

Additional information on the EFC, its structure and objectives is available on the EFC website: www.europeanfinanicialcoalition.eu

Colophon
Text: European Cybercrime Centre (EC3) – Europol
Responsible editor: European Financial Coalition against Commercial Sexual Exploitation of Children Online

With the financial support of the Prevention of and Fight against Crime Programme
European Commission –Directorate-General Home Affairs

Contents

With the financial support of the Prevention of and Fight against Crime Programme
European Commission –Directorate-General Home Affairs

1. Introduction & Executive Summary

The aim of this report is to provide an update to the *Strategic Assessment of Commercial Sexual Exploitation of Children Online* published in October 2013 in the framework of European Financial Coalition (EFC). In addition to presenting the 2013 facts and figures, it also looks at other essential factors in this area. There is a lack of a globally agreed definition of commercial Child Sexual Exploitation (CSE), inherent difficulties in creating one and individual working definitions may be more appropriate in a case-by-case assessment due to cultural, legal or procedural limitations. This has implications for organisations or projects dealing with the assessment of such content[1] and also impacts on the response to hotline notifications in Law Enforcement Agencies (LEA) in the European Union.

This assessment also makes a clear distinction between the situation on the Surface Web[2], the Deep Web[3] and the Darknet[4]. The purpose of this is to influence an outdated assessment of the problem, which characterises commercial CSE as dedicated websites or URLs being accessible by regular search engines. Moreover, this stereotype will also be examined by providing facts relating to emerging trends and new forms of commercial activities on the Surface Web itself.

Through an examination of the scale and extent of existing activity as well as the most recent developments in these areas, this assessment aims to recommend solutions and suggest regulations. These are aimed at enabling both the Law Enforcement (LE) and private sector communities to prevent and tackle this horrific crime in the best possible way.

Following the example of the 2013 assessment, this report consciously follows a more qualitative approach to analysing commercial aspects of online CSE. Careful attention was also paid to quantitative data whenever available. In qualitative terms the research heavily draws on the observations of online child sexual exploitation investigators themselves. Between April and May 2014, interviews were conducted with 18 experts[5] in the child sexual exploitation field, actively participating in operational undertakings of Europol's European Cybercrime Centre

---

[1] *INHOPE is an active and collaborative network of 51 hotlines in 45 countries worldwide, dealing with illegal content online and committed to stamping out child sexual abuse from the Internet.*

[2] *Surface Web – indexed by standard search engines.*

[3] *Deep Web – World Wide Web content that is not part of the Surface Web.*

[4] *The Darknet –'A collection of networks and technologies used to share digital content. The Darknet is not a separate physical network but an application and protocol layer riding on existing networks. Examples of Darknets are peer-to-peer file sharing, CD and DVD copying and key or password sharing on email and newsgroups'.*
Definition provided by Peter Biddle, Paul England, Marcus Peinado, and Bryan Willman in 'The Darknet and the Future of Content Distribution'; http://crypto.stanford.edu/DRM2002/darknet5.doc.
For the purpose of this assessment the term Darknet will be used, and it should be understood as 'web communications and technologies most commonly associated with illegal or dissent activity, where connections and sharing are anonymous'.

[5] *Experts who took part in the interviews come from Belgium, Bulgaria, Denmark, Germany, Ireland, Italy, Netherlands, Norway, Poland, Romania, Slovenia, Spain, Sweden, Switzerland, UK as well as the US (FBI).*

(EC3)[6]. Furthermore, additional information was simultaneously collected in order to produce the 2014 Internet Organised Crime Threat Assessment (iOCTA)[7], the document examining and reporting the current threat landscape across the whole of the EU for all cyber-dependent and cyber-enabled crime areas. Additionally, to make the response of LE complete, this assessment refers in many instances to expertise gathered by the members of FP Twins[8].

This report is also based on the expertise of members of the EFC[9], who answered specific data collection templates individually prepared and addressed to them by Work Package 2 (WP2) leads EC3 and INHOPE.

Combined with open source research and analysis, all the above mentioned contributions have been invaluable to the production of this assessment. WP2 leads would like to express their thanks to all members of the international community for their cooperation.

Based on the information available to WP2 in November 2014, key findings are as follows:

- *The evolution of commercial CSE online requires a new working definition, which would enable all stakeholders to set up standards for what needs to be monitored and actioned;*
- *There is a definite change in the traditional distinction between non-commercial and commercial distribution, which branded the former as largely profit driven, and conducted by those with limited sexual interest in children. Individuals with a sexual interest in children who produce and distribute child abuse material are becoming more entrepreneurial. This process of change is heavily driven by the search for new and novel materials, and it is believed to refer more specifically to users of the Darknet;*
- *The live streaming of abuse for payment is no longer an emerging trend but an established reality. It is of particular concern in the context of emerging markets due to Internet adoption there;*
- *As there are new forms of online behaviour – such as commercial sexual extortion – there is a real risk that more entrepreneurial offenders will replicate this business model;*
- *Although the scope of commercial activities in the Deep Web and the Darknet are still limited in comparison to the Surface Web, they deserve greater attention. The kind of material that is being commercially traded can be of a 'tailor made' nature, created on demand, and can therefore lead directly to further hands-on abuse. It can furthermore provide a source of intelligence about payment mechanisms which are discussed there;*

---

[6] *The European Cybercrime Centre is hosted by Europol - the European law enforcement agency in The Hague, the Netherlands.*
[7] *https://www.europol.europa.eu/ec3*
[8] *The team of experts and analysts dealing with CSE in the European Cybercrime Centre (EC3).*
[9] *INHOPE, IWF, CEOP, VISA, MasterCard, PayPal, Western Union, Web Shield, G2, GSMA, Google, Microsoft, ICMEC.*

With the financial support of the Prevention of and Fight against Crime Programme
European Commission –Directorate-General Home Affairs

- *There is a clear shift from traditional credit card payments to the ones providing the most anonymity, namely alternative payment options, including virtual currency. The Internet Watch Foundation (IWF)[10] analyses point to money transfers and Bitcoin[11] as the most recommended payment methods offered by new brands identified within the Website Brand Project[12]. This indicates that there is a need in this market for functioning and reliable payment systems;*
- *There has been a marked increase in the abuse of legitimate hosting services for the distribution of Child Abuse Material (CAM). Online services such as cyberlockers[13] are used by entrepreneurial offenders to distribute CAM for financial gain. It is advisable to monitor the abuse of Affiliate/Rewards Programs and Pay-for-Premium Services;*
- *The use of hosting and live streaming services for commercial CSE is a trend requiring proper countermeasures, (such as hash and photo DNA oriented initiatives), enabling providers to introduce procedures for identifying and mitigating the spread of CAM. Discussion on a more proactive approach or even on regulation of this area should take place;*
- *Significantly, the list of countries registered by INHOPE for hosting commercially distributed CAM sees the addition of two new countries in the top 10: Luxembourg and Singapore. In 2013 the most misused services were located in: the USA, the Netherlands, the Russian Federation, Japan, Ukraine, Canada, the Czech Republic, Germany, Luxembourg and Singapore. Kazakhstan and Hungary mentioned last year in the top 10 group are still reported but with a smaller number of reports;*
- *Analysis by the Internet Watch Foundation discloses that of the top 10 most prolific commercial CAM distribution brands active during 2013, 8 were apparently associated with a single Top Level Distributor (TLD). These 8 account for 15% of the total commercial content on the Surface Web. Furthermore, of 575 brands produced by 8 TLDs in 2013, 347 (60%) were previously unseen. This seems to confirm last year's findings that while there are large numbers of URLs being used for the commercial distribution of CAM, these can be attributed to a small number of extremely prolific Top Level Distributors*

---

[10] Internet Watch Foundation is the UK hotline belonging to INHOPE's network for reporting criminal online content (child sexual abuse content hosted anywhere in the world, criminally obscene adult content hosted in the UK, non-photographic child sexual abuse images hosted in the UK).

[11] Bitcoin is a decentralised virtual peer-to-peer (P2P) currency.

[12] Website Brands Project was initiated by the IWF in 2009 in order to attempt to quantify the true volume of commercial websites in operation, and by extension the number of Top Level Distributors which may be responsible for the creation and operation of the websites.

[13] A 'cyberlocker' in this report should be understood as a third-party online service that provides file-storing and file-sharing services for various types of media files and data, including a service that requires a premium account to download either faster or simultaneously. Such services are also called one-click hosters.

2. Definition of Commercial Child Sexual Exploitation Online

It is known that there are varying legal definitions of CAM, what is more likely however to cause difficulties due to definition inconsistency, is the understanding of what is commercial or not.

As highlighted in the report published in October 2013, new material is a currency in itself. In the framework of the EFC, the focus is on the distribution of content that brings financial gain to its provider. However, even this hypothesis may fall short in including the currently available methods of gaining commercial benefit from content distribution. Do we only consider commercial content that becomes available through direct transactions? Does this include cyberlockers that, although they normally provide free services, their uploaders may require a premium account from which they will receive a commission for downloads? What if the payment page only acts as an identity theft mechanism but does not provide access to CAM?

These questions, among others, constitute real obstacles in clearly defining what is currently considered to be commercial.

2.1. Available terminologies

The EFC 2009-2010 report, which was produced during the time of CEOP's lead on the project, suggested the following definition: *'The use of the word commercial refers to child abuse images that are available to purchase. This could include a website designed to provide child abuse images for a cost (normally subscription) or uncensored newsgroups who charge a fee for membership and have child abuse images available as part of their service'.*

Although newsgroups may no longer deserve the same prominence, this definition could now be extended to the re-selling of images, or requiring paid access to online facilities such as linked pages or cyberlockers, which can be used by offenders to store or distribute their images.

The only recent definitions of commercial content and websites are provided by the IWF. Actionable content will be considered by them to be *commercial* if '*in the professional opinion of the Internet Content Analyst, the purpose for which it was created or the purpose for which it is being used is intended for commercial gain'*, whereas a commercial website *'is any website which provides or appears to provide paid access to child sexual abuse images either directly through a payment page or indirectly through a series of linked pages' (Note: a commercial website can be hosted within a larger free-hosting or website)*[14].

---

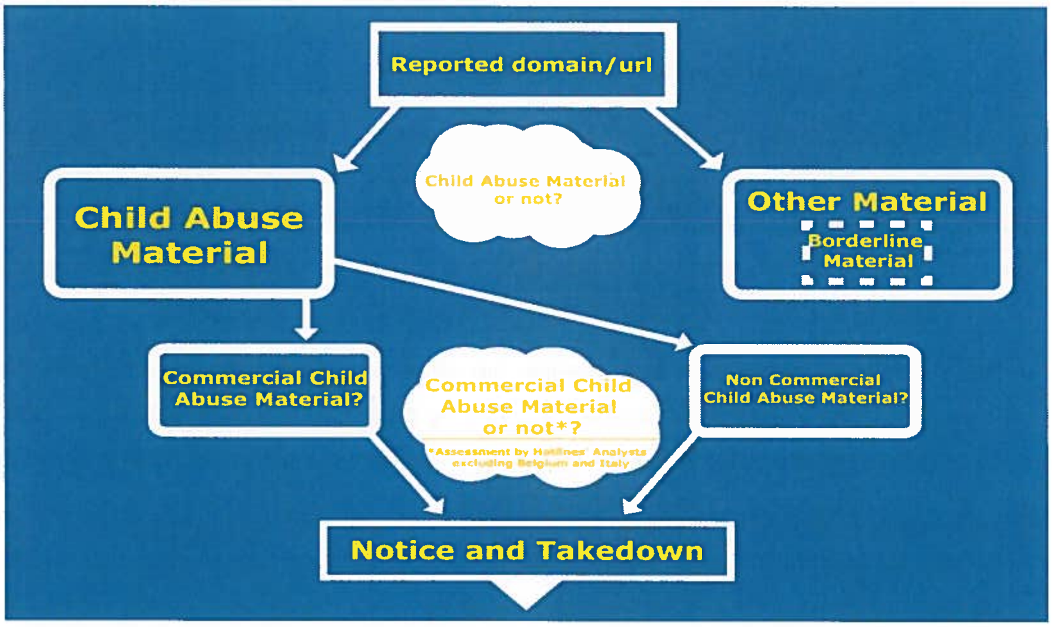
[14] *IWF Briefing Paper – Website Brands Project, March 2013.*

INHOPE defines a 'commercial' website as '*any website which provides or appears to provide paid access to child sexual abuse images either directly through a payment page or indirectly through a series of linked pages*'[15].

None of the above mentioned definitions cover the full spectrum of current forms of commercial CSE online. Such a gap means in turn that classification needs to take place on a case-by-case basis. This approach, enhanced by existing inconsistencies in legal frameworks or agreements between hotlines and the LEA across the world could result in discrepancies in building a complete picture of commercial CSE online.

2.2. Related issues – process of assessment

INHOPE and its members have elaborated the Notice and Takedown process where illegal content is removed from public access. The essential part of this action is a proper assessment of the content as presented below:



Given the fact that INHOPE's activities span many jurisdictions[16] and therefore use different interpretations of what is commercial, the organisation reports that the lack of consistent and generally accepted terminology is a global issue. The interpretation will also largely rely on the analyst's experience and subjective approach. Along with projects and initiatives such as the EFC, INHOPE is working with its members to address this concern.

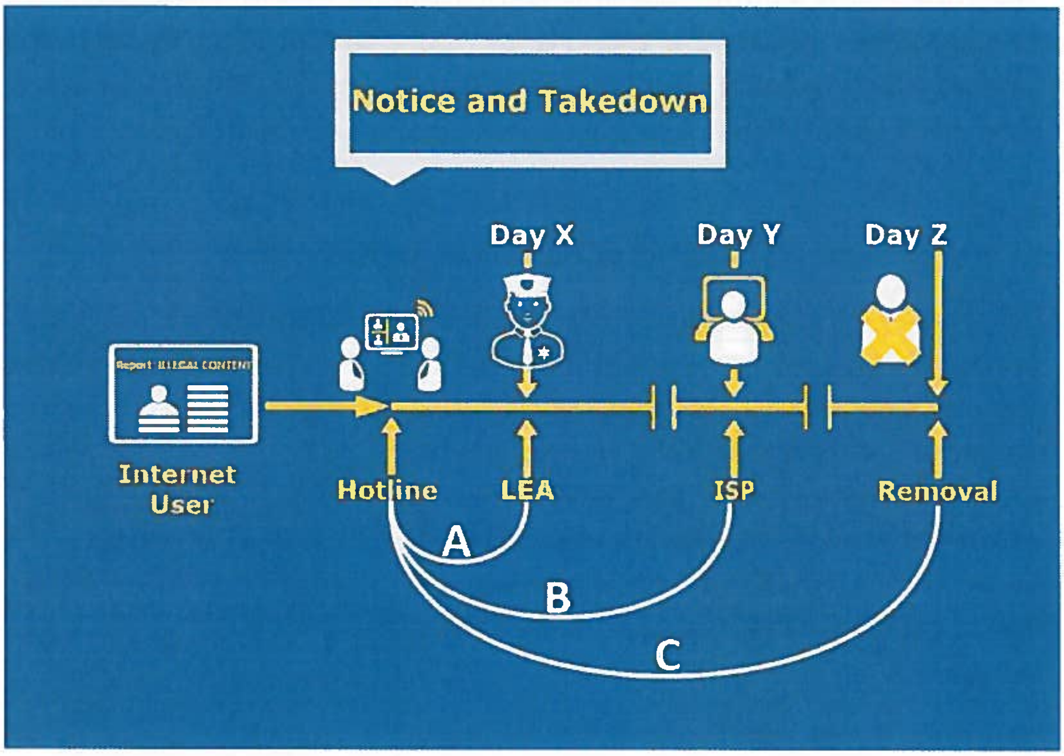
---

[15] *INHOPE's working definition provided at the beginning of 2013 and meant for the work of EFC Work Package 1.*
[16] *At the time of writing, INHOPE coordinates a network of 51 hotlines in 45 countries across the world.*

With the financial support of the Prevention of and Fight against Crime Programme
European Commission –Directorate-General Home Affairs

At present, INHOPE hotlines mainly collect information regarding known or traditional payment methods, leaving aside a wide pool of 'not determined' ones, whereas in the light of recent developments it is of the utmost importance to pay attention to newly emerging ones.

As far as the exact Notice and Takedown process is concerned, INHOPE and its members usually[17] follow the following scheme:



Once the report is received and assessed by the hotline as CAM under their jurisdiction, it will normally be forwarded to the LEA (Process A above) and/or[18] the Internet Service Provider (ISP) (Process B). Content removal performed by a Content Service Provider (Process C) will follow where appropriate.

The existing system seems to be very effective in removing illegal content from the network. In 2013, 97% of reports were forwarded to the LEA within 1 day[19]. INHOPE also announce content

---

[17] Processes may differ between hotlines across the world based on their legal status, national law, as well as an agreement with LEA. The process in the picture illustrates the most common approach.

[18] In some cases both LEA and ISP will be informed at the same time, whereas in other cases there will be a delay between the LEA and ISP.

[19] INHOPE Facts, Figures & Trends, http://inhope.org/Libraries/Infographics/INHOPE-2013-Inforgraphic.sflb.ashx

With the financial support of the Prevention of and Fight against Crime Programme
European Commission –Directorate-General Home Affairs

removal times in the Member States of 80% within 3 days - a significant improvement on 56% in 2012[20].

However, there are several shortcomings in this mechanism. The only way to check the advertised payment system is to conduct test transactions which are not only restricted to LEA but also cannot be carried out in all EU MS due to different national legislations. Furthermore, a response by the LEA also depends on the kind of information collected, and the way in which it is submitted, as it should either trigger the new case or serve as intelligence. Also, reports which are less than a day old are difficult to investigate since the sites may no longer be active. In the current situation there is a risk that valuable information may be lost during this process.

3. Scale and Extent of Commercial Distribution – the Surface Web

Differences in the assessment of whether the reported material should be considered as commercial CAM or not, as well as difficulties in verification of the advertised payment method does not really assist in drawing a real picture of commercial CAM distribution online. However, it is no easier to collect quantifiable information in the LE environment, where the data related to various forms of online CSE is not always recorded at national level. Even if this is the case, collection methods differ nationally.

> **Case study:**
> **IWF reports that several of the most prolific distributors identified in the website brands project also package 'child modelling' website templates on the same domains as their CAM brands.**

Additionally, it has been observed that the initial response of some specialists dealing with CSE to the question about the scale of commercial CAM distribution online is driven by a somewhat outdated way of thinking. In many cases, they identify the Surface Web based websites as its main form, excluding in the first instance other forms of commercial activity in today's digital world, such as live web streaming and the situation in the Darknet.

3.1. Latest figures

The situation as it was highlighted in the 2013 report, that the vast majority of CAM is still distributed non-commercially on the Surface Web using peer-to-peer (P2P) technologies is still a reality but commercial distribution still persists there.

[20] *http://cdn.pressdoc-static.com/33629/documents/19230-1369212176-INHOPE_Annual_Report_2012.pdf*

With the financial support of the Prevention of and Fight against Crime Programme
European Commission –Directorate-General Home Affairs

There is also no change in the assessment of the situation by representatives of EU LE specialists. Eighteen experts participating in the interviews confirmed that, in their opinion, a very small amount of CAM is now paid for. The wide availability of new material in non-commercial environments and successful countermeasures implemented by the private sector was cited by many experts as a reason for this.

The same experts responded to a survey connected to the production of the iOCTA. In answer to a question on how many cases of commercial CAM distribution online they had encountered in the period from September 2012 until the 1st quarter of 2014,[21] they mentioned none, 1 to 2, or several cases.

In 2013, INHOPE member hotlines registered 5236 URLs of suspected commercial Child Sexual Abuse Material that were in turn referred to Europol[22] for further analysis. This number accounts for 13% of reports that INHOPE hotline processed as commercial, with 87% of reports in the network being assessed as non-commercial[23]. It seems that the number of reports of a commercial nature in the last three years is growing, although the data set available to WP2 leads within the EFC project is not yet complete[24].

INHOPE	October - December 2012	January - December 2013	January - June 2014
URLs suspected of commercial distribution	1138	5236	2940

It is worth highlighting again that according to findings revealed by the IWF under the Website Brands Project, the same websites would often appear on multiple URLs over a period of time. Therefore, the number of URLs actioned for containing commercial CAM is not necessarily an accurate reflection of the number of commercial websites which may actually be in operation. Additionally, there were numerous links between the different sites which suggested that groups of brands may be operated by single overarching entities (TLDs).

---

[21] *Ireland, Denmark, Luxembourg, Greece, Sweden, France, Hungary, Croatia, Cyprus, Czech Republic, Slovenia, Serbia, Germany, Finland, Macedonia, Montenegro, Slovakia, Spain, Italy.*

[22] *A Memorandum of Understanding (MoU) was signed between INHOPE and EC3, which enables EC3 to receive - via an automated service developed by INHOPE - the URL reports from INHOPE's database pertaining to commercial CAM distribution websites on a daily basis.*

[23] *INHOPE Facts, Figures & Trends.*

[24] *The reported date range covers period from October 2012 until June 2014.*

The IWF's ongoing analysis suggests that suspicious websites are operated by a small core group of criminal entities. The total number of brands identified since 2009 was more than 1609[25] of which 575 brands were active in 2013, whilst 347 (60%) of these were previously unseen. This is slightly more than in 2012 when 513 individual brands were active, and 268 new brands were created during the course of the year. However, a large proportion of these new brands were variations on previously seen templates as opposed to completely new templates. The content on all these templates is largely well-known and recycled content. Of the top 10 most prolific brands active during 2013, 8 were apparently associated with a single TLD and account for 15% of the total commercial content.

To complete a picture of commercial CAM distribution online, especially one which is associated with an 'old-fashioned way of thinking' it is worth referring to so-called modeling sites, as there is evidence that commercial CSE is very often linked to so-called modeling sites. Child modeling material which, under the legislation of certain EU Member States is assessed as CAM, can be hosted legally in other states where it is not considered to be of an illegal nature. As reported by INHOPE's hotlines this type of material is also often found on home pages of commercial websites offering illegal material in exchange for a paid subscription. Child modeling sites frequently operate on the same domain as, or are hyperlinked with, the most prolific CAM websites. A large number of children depicted in images on the child modeling sites are victims also known to appear in CAM images.

3.2. Existing patterns in commercial distribution. Web distribution and hosting

Although there is evidence that commercial distribution of CSE online is evolving, there are stable patterns which have not changed. Meeting environments such as Bulletin Board Systems (BBS), social media and closed forums still facilitate direct communication and distribution of links. Those links are to content stored on bulletproof hosting sites or in encrypted online storage facilities, as well as a limited amount of public photo sharing sites.

According to IWF the dedicated domain is still the preferred method of distributing CAM by the most prolific Top Level Distributors identified under the Website Brands Project. As already noted, numerous

Case study: Although the IWF cannot pass payment barriers, they frequently action forums which contain numerous thumbnails of CAM with associated links to a premium only download of the full file from a third party cyberlocker. Whilst it is not possible to assess the content on these premium access only cyberlockers as CAM, it is extremely likely that the content does consist of CAM as advertised.

[25] *Up to May 2014.*

With the financial support of the Prevention of and Fight against Crime Programme
European Commission –Directorate-General Home Affairs

brands are hosted on the same domain, for example the most prolific distributor hosts approximately 7 different brands per domain.

Interesting observations come from INHOPE as their analysis demonstrates that many domains appear to be moving hosting providers, or abusing multiple providers at the same time.

The high number of ISPs associated with certain domains reveals the extent of abuse of these domains, even if individuals can register free domains and then point DNS records to them while hosting the content anywhere. It is also interesting to note the overlap of both countries and ISPs that seem to host these two most-reported domains.

Another interesting observation recorded by INHOPE is that of the commercial reports in this section, banner sites[26] account for more than 30% and file hosting services[27] for 7%.

In 2013, the IWF observed the re-emergence of hacked sites as a distribution method, when two templates were distributing images and malware on a number of hacked legitimate small business and personal websites. It was believed from the nature of the malware, folder names and site types targeted, that those two templates were associated with a single distributor and that the primary motivation was not distribution of CAM but distribution of the malware.

In 2014, the IWF encountered new Top Level Distributors (TLDs) using hacked sites to provide access to CAM. The initial distribution method is to send a URL in a spam email which clearly advertises itself as CAM. Additionally, these sites purport to accept payment only in Bitcoin.

Since 2011, the IWF have observed increased use of a technique of using 'disguised websites'[28] to distribute CAM and defraud legitimate payment providers by annihilation of their compliance procedures. In 2013, the referrer sites were increasingly being used to provide direct access to the most prolific commercial child sexual abuse websites which have been identified as a part of the Website Brands Project. This technique represents a challenge to successful removal as hotlines are not able to proceed with the Notice and Takedown without knowledge of the referring URL. INHOPE reports that this challenge can become even greater with referrers sometimes expiring after a certain period of time. When dealing with multiple time zones as the INHOPE network does, it may be that even if the referrer is reported to another hotline or to law enforcement for investigation, it may have expired and a new referrer URL is necessary to display the content.

---

[26] As per INHOPE's working definition, banner sites link to other sites meaning when the user clicks on a banner image, it opens the linked website. Usually banner sites are partially or fully automated and act as the traffic generator or advertisement platform. Commercial sites are usually advertised through banner sites, link sites and forums.

[27] These are hosting services specifically designed to host user files.

[28] These websites present different content depending on the route the user takes to reach them. When the URL is loaded directly into the browser, the page which loads contains legitimate adult content. However, when accessed via a particular gateway site (referrer) the page displays child sexual abuse content.

With the financial support of the Prevention of and Fight against Crime Programme
European Commission –Directorate-General Home Affairs

A dynamic shift in hosting trends in recent years has created an additional challenge for the successful combating of the online distribution of CAM. In particular, it is evidenced by the IWF in their annual report that there has been a marked increase in the abuse of legitimate hosting services for the distribution of CAM. In 2013, 10 695 URLs were hosted on free hosting services, 2445 URLs were in paid hosting services, and 36 URLs on hidden services[29]. 2183 reports (68%) of the commercial content actioned were using paid hosting on a dedicated domain[30].

While analysing online hosting of CAM it is worth emphasising again the increase of illegal content, including CAM, being sold through cyberlockers.

An analysis conducted by G2 Web Services[31] on a specific set of 16-21 cyberlockers over 15 weeks, identified that 25% of them contained CAM, and that CAM is most likely hosted on cyberlockers that offer some sort of premium upload/download service[32]. In general, both so-called Pay-for-Premium Services[33], as well as Affiliate/Rewards Programs[34] possess those vulnerabilities, which can be misused by offenders interested in the distribution of CAM for financial gain.

The IWF reports that it continues to be the case that as new cyberlocker services come online, they are abused for the storage of CAM. This reinforces evidence that there has been a marked increase in the use of cyberlockers to host CAM, from 649 instances in 2012 to 1400 in 2013. Also, it is worth noting that selling passwords for access to online storage sites as a method of commercial distribution has been in operation for some time.

According to INHOPE the vast majority of cyberlockers that had reports for commercial activity in 2013 were located in the Netherlands.

3.3. Analysis of Commercial URL data provided by INHOPE

A total of 5236 URLs suspected of the commercial distribution of CAM in 2013 divided into hosting countries[35] (for countries with more than 20 reports) as follows:

---

29 https://www.iwf.org.uk/accountability/annual-reports, P 12 and 17.

30 It is worth highlighting that cyberlocker content - where there is an option to download more quickly using a premium account - is not classified by IWF as commercial at this time.

31 G2 Web Services is a provider of payment risk management solutions in due diligence, compliance, and fraud protection.

32 Contribution by G2 Web Services.

33 Premium Services offer their users additional features, such as increased download/upload speed, simultaneous download etc. Access to certain files can also be limited unless a user pays for a premium service.

34 Affiliate/Rewards Programs allow users who upload content to earn a portion of the revenue their uploads generate.

35 It is important to emphasise that tracing hosting countries relies on tools that identify locations based on IPs registered to hosting servers. With the increase of cloud hosting and due to its distributed nature, the proxy and network privacy solutions associated with cloud computing as well as Content Delivery Networks, it is safe to say that the possibilities of accurately tracing content using the currently available tools will decrease.

With the financial support of the Prevention of and Fight against Crime Programme
European Commission –Directorate-General Home Affairs

INHOPE Commercial URLs by hosting country	2013
1. United States	2617
2. Netherlands	942
3. Russian Federation	437
4. Japan	322
5. Ukraine	182
6. Canada	177
7. Czech Republic	125
8. Germany	81
9. Luxembourg	77
10. Singapore	60
11. Korea, South	51
12. Kazakhstan	42
13. United Kingdom	34
14. France	27

This distribution is broadly similar to INHOPE statistics in the two other periods:

The hosting countries (for countries with more than 20 reports)	October - December 2012	The hosting countries (for countries with more than 20 reports)	January - June 2014
1. United States	516	1. United States	2048
2. Russian Federation	121	2. Japan	455
3. Kazakhstan	119	3. Netherlands	156
4. Japan	83	4. Russian Federation	88
5. Netherlands	67	5. Ukraine	59
6. Ukraine	58	6. Canada	23
7. Germany	50	7. Germany	22
8. Czech Republic	40		
9. Hungary	24		

By drilling down into the country results the most prolific hosters may be identified.

In the available data for hosting countries, 'Europe' appears as a country. This invalid hosting country appears often in the case of the company CloudFlare, which provides a legitimate network privacy/security solution to obfuscate their clients' IPs. But as with the majority of legitimate services, this solution seems to be abused for the distribution of CAM[36]. A network solutions company (not an ISP) appears as the second most reported provider in the US, but was not on the list of the previous WP2 Strategic Assessment Report.

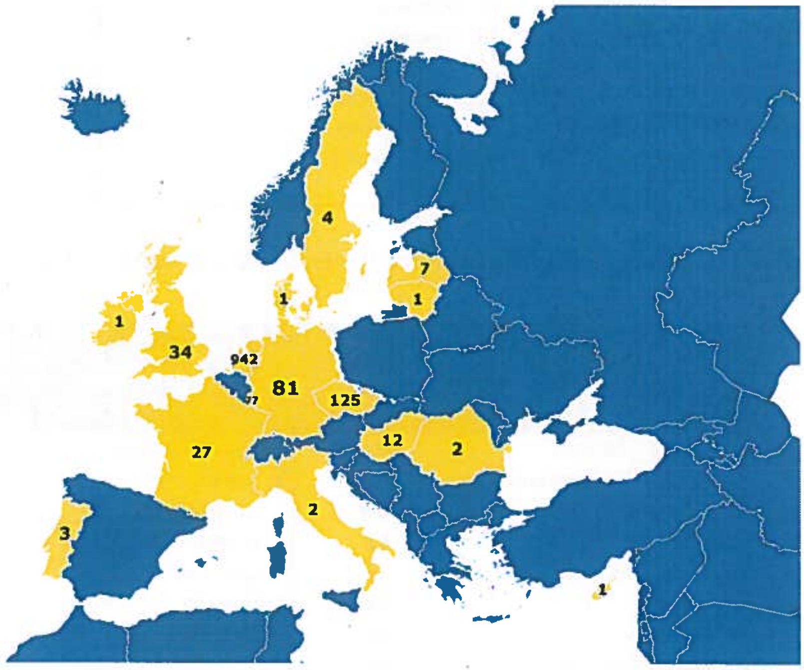
[36] *INHOPE has observed a high number of URLs that, although they seem to be associated with CloudFlare by tracing tools with hosting country the United States, this tracing appears to be incorrect. A solution for this problem is based on communications with its US Member CyberTipline, to which CloudFlare is obliged by federal law to report the abuse on their services along with the actual IP of the relevant server. Once the real locations have been traced, INHOPE hotlines in the hosting country will receive the report for further action.*

With the financial support of the Prevention of and Fight against Crime Programme
European Commission –Directorate-General Home Affairs

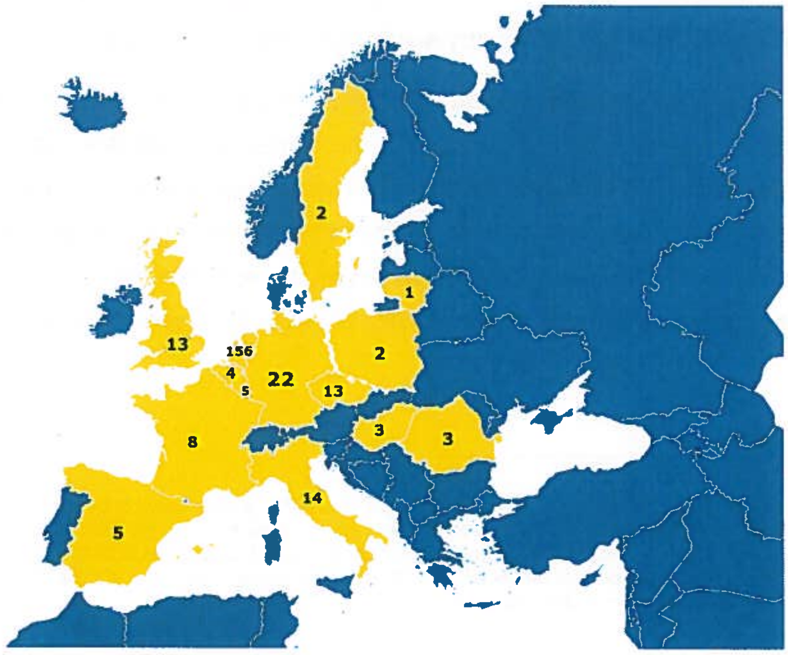
Also, the fact that a number of the most-reported providers above belong to some of the most popular hosting services in the world indicates that a large amount of commercial content is distributed by misusing legitimate companies.

Number of commercial URLs by hosting country in October – December 2012

It is also interesting to have a closer look at the reported hosting countries in the EU.



Number of commercial URLs by hosting country in 2013



With the financial support of the Prevention of and Fight against Crime Programme
European Commission –Directorate-General Home Affairs

Number of commercial URLs by hosting country in January – June 2014

The above reveals that the EU countries hosting the largest number of URLs suspected of the commercial distribution of CAM in the reported period of time (October 2012 – June 2014) are - in descending order - Netherlands, Czech Republic, Germany, Luxembourg, United Kingdom, Hungary and France.

The table below shows the number of ISPs per country (for countries with more than 2 ISPs) suspected of hosting commercial CAM.

Hosting Country	# of ISPs (>2)
United States	115
Russian Federation	35
Netherlands	27
Ukraine	23
United Kingdom	20
Germany	11
Japan	11
Czech Republic	6
Korea, South	5
Canada	5
Luxembourg	3
Latvia	3
Total	264

It seems that all forms of 'traditional' commercial distribution are well recognised, primarily by the effective system of the Notice and Takedown, therefore more attention should be given to its new forms, such as commercial web streaming, sexual extortion, as well as paid access to previously unseen, quite often 'on demand' material, in environments like Tor[37].

4. Expanding trends within commercial CSE online

Technological expansion, growing Internet coverage, widespread availability of mobile devices – are all factors constantly transforming our society into a digital one. Without doubt, no-one had prepared us and our children to cope with these challenges. While the ultimate consequences of such rapid technological and social developments will only be known in the future, there is enough evidence to say that harm has already been done.

[37] *Tor -The Onion Router - is free software for enabling online anonymity and resisting censorship.*

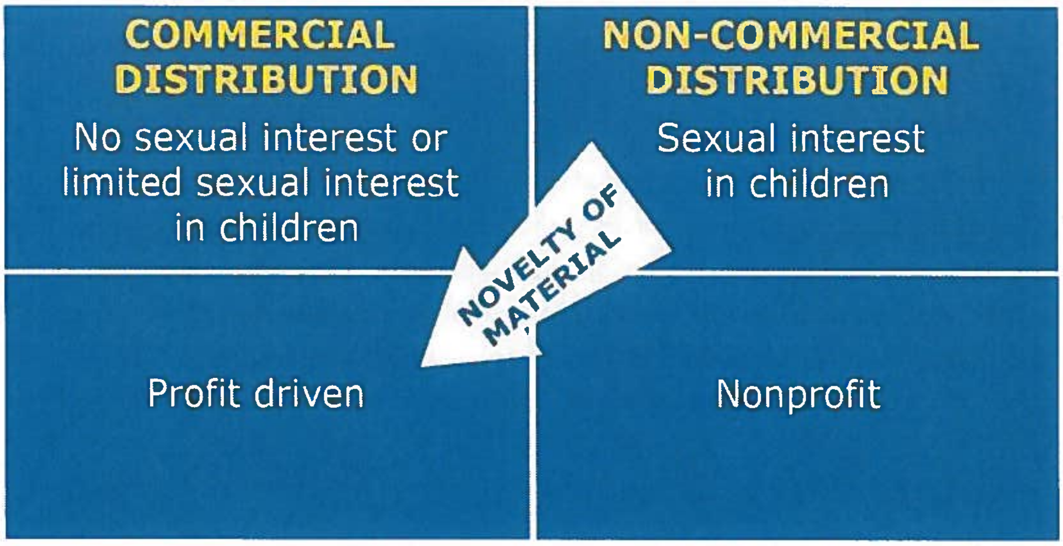
As highlighted in the introduction of this report, one of its aims is to widen the understanding of online commercial CAM distribution. The dynamic nature of this crime area dictates that expanding trends should always be taken into consideration whenever questions about the current scale of this phenomenon arise. Some of those trends are explored now.

It is now understood that both individuals with limited sexual interest in children, as well as those having an interest in producing and distributing CAM, are becoming more entrepreneurial and are exploiting technological developments for financial profit.

The previous report brought to its readers' attention a further evolution of commercial distribution based on a commercialisation of those forms of CSE that had so far been more typical of non-commercial distribution as well as new models of this phenomenon. The report challenged the traditional distinction between commercial and non-commercial distribution, which branded the former as largely profit driven, and conducted by those with limited sexual interest in children.

In this sense developments such as profit driven blackmailing of children to disseminate indecent materials depicting them, as well as the commercial distribution of images and videos obtained through online solicitation and as self-generated indecent material, should be taken into consideration. In addition, new instances of commercial distribution in the Darknet are evidenced.

Although ancillary research would be necessary to explore the background of this phenomenon, it is already known that a process of further evolution of commercial CAM distribution is heavily driven by the novelty of materials as explained below:



With the financial support of the Prevention of and Fight against Crime Programme
European Commission –Directorate-General Home Affairs

4.1. Self-generated indecent material and commercial sexual extortion

The expression 'sextortion'[38] was previously used in the 2013 report, and explained as the popular term for the process by which young people are coerced into producing indecent material by the threat of exposure. Offenders use different tactics in order to contact young people. While in-depth analysis of the background of sexual extortion goes beyond the scope of this research, it is worth mentioning that in some instances such processes may be triggered by self-generated indecent materials which are in circulation on social media.

There are several reasons why this phenomenon is being exploited by online predators. Not surprisingly one of the most significant ones, apart from power and control, seems to be the novelty of 'home-made' material. This can, in some instances such as a gateway to restricted areas, be a currency in itself.

Sexual extortion as a modus operandi may also attract individuals looking for easy financial gain. This can take the form of either commercial distribution of materials obtained through online solicitation or blackmailing of victims by demanding money for not distributing the indecent materials. Such a trend shapes a somewhat different understanding of the scope of this phenomenon than the one known so far, and points to a new term such as 'commercial sexual extortion'.

Although only one year has passed since the last report, which highlighted an increasing trend of commercialisation of new forms of CSE, there is concerning evidence to suggest that a retail market for the above mentioned forms already exists, and is developing.

An increase in the number of websites which had apparently been created specifically to display self-generated sexually explicit images and videos featuring young people had been seen by the IWF for some time. However, in 2013 the IWF saw a commercial child sexual abuse website offering the sale of self-generated sexual images and videos of young people.

Case study: In July 2013 a 17-year-old boy died when he threw himself from a bridge near Edinburgh. He had been targeted online by an offender who posed as a teenage girl and with whom he shared indecent images of himself. The victim was then blackmailed by the offender demanding money. If he failed to pay he would post the victim's naked images on social networking sites.

[38] *The correct term suggested by specialists dealing with CSE for this crime type is 'sexual extortion'.*

With the financial support of the Prevention of and Fight against Crime Programme
European Commission –Directorate-General Home Affairs

Some recently reported case studies present a truly broad spectrum of criminal behaviour.

In a recent investigation a suspect that was arrested in January 2014 used more than 80 social networking profiles, email addresses and video chat accounts to sexually abuse children via web cams. Once victims had sent him the indecent image or video of themselves, he started threatening them and involving them in far more serious abuse. The youngest child was an 8-year-old girl, who was forced to involve other children in the abuse. The same suspect, who pretended to be a 13-year-old boy, also coerced adult men into performing a sexual act via web cam which was recorded and used against them unless they paid certain amounts of money. Unfortunately, it is not known at the time of writing if indecent materials provided by the children were commercially distributed online, but bearing in mind the profile of the suspect this possibility should not be excluded.

In another case a 17-year-old girl was a victim of extortion which started when her boyfriend took a photo of her breasts with his mobile phone, and shared it with his 17 year old friend. The latter sent this photo via a social media platform to the victim to inform her he had it, demanding money from her and threatening her with publishing her photo elsewhere if she refused to pay him. Verbal blackmailing also took place at school. Since the girl was afraid that he would publish the photo on the Internet, she gradually began to give him money to the amounts of EUR 10 or 20, which totalled approximately EUR 600 over a few months. Although the demand for more obscene material has not been expressed in this case, it shows a certain evolution of profit driven extortion linked to self-generated indecent material.

Some interesting differences have been observed between cases of non-commercial sexual extortion and the ones where online coercion was driven by financial gain. While the first kind of such criminal performance will be more likely a one-man activity, the latter one can be considered as a potentially lucrative business opportunity, where large scale sexual extortion schemes would be applicable.

A good example of large-scale sexual extortion is a combination of the web cam scamming with blackmail which usually takes place on dating sites, in chat rooms, or social networks. Once contact is established it is moved towards web cam contact where the contacts are secretly filmed engaging in sexual practices. The victims are then blackmailed and forced to make money transfers to the perpetrator to prevent the videos from being distributed. The scale of these purely profit driven sexual extortion networks is tremendous. No attention is given to victims, who are only a means to collect more money in this semi-automated process.

There is some evidence pointing to a ring of African states in addition to the Southeast Asia-based networks that are targeting victims throughout Europe.

With the financial support of the Prevention of and Fight against Crime Programme
European Commission –Directorate-General Home Affairs

One recent international operation coordinated by Interpol led to the identification of between 190 and 195 individuals working for organised crime groups operating from the Philippines, and resulted in 58 arrests. Close cooperation of the international LE community led to the identification of sexual extortion victims in Indonesia, the Philippines, Singapore, the United Kingdom and the United States. Potential victims were also traced to Australia, South Korea and Malaysia in addition to the hundreds of individuals in Hong Kong and Singapore already reported as victims.

Operating on an almost industrial scale from call centre-style offices, such cyber-blackmail agents are provided with training and offered bonus incentives such as holidays, cash or mobile phones for reaching their financial targets[39].

Some sources refer to such cyber-café criminals as the latest incarnation of the infamous Nigerian '419' Advance Fee Fraud scam. In the past decade these have mutated into a massive Internet-based operation, causing difficulties for international police authorities, Nigerian fraud suppression squads and Internet providers whose servers are spammed by millions of misleading messages daily[40].

It is important to mention that although the Directive 2011/93/EU[41] introduced provisions on the Solicitation of children for sexual purposes (Article 6), prosecution very much depends on the age of sexual consent, which varies in the EU MS from 13 to 17. This means that in some cases obtaining indecent photos or videos through online solicitation would not be punishable, which leaves quite a big gap for such materials to go into worldwide circulation.

4.2. Commercial Live Web Streaming

As has already been highlighted, the live streaming of abuse for payment - Live Distant-Child Abuse (LDCA)[42] - is an established trend. It is a fact that needs to be duly acknowledged by all stakeholders who could contribute to the successful tackling of this particular type of crime. The likelihood that this threat will increase during the next one to three years is foreseen by the National Crime Agency in the UK[43].

Live streaming can be a part of a sexual extortion process, although for the purpose of this document it should rather be considered as a separate activity, carefully arranged as well as involving money transfers in most of the cases. This criminal activity is based on members of

---

[39] http://www.interpol.int/en/News-and-media/News/2014/N2014-075

[40] http://www.french-news-online.com/wordpress/?p=13706#axzz2chHjoZh9

[41] Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA.

[42] The term suggested by Europol's Focal Point (FP) Twins team

[43] National Strategic Assessment of Serious and Organised Crime 2014.

With the financial support of the Prevention of and Fight against Crime Programme
European Commission –Directorate-General Home Affairs

networks who control access to the children. These persons offer homeless children or children from their own family for sexual abuse by individuals live in front of a camera in the EU, or other developed countries, for financial gain.

Exhaustive analysis of the nature of this phenomenon is outside of the scope of this report but it is important to underline that LDCA is often unfairly considered as a 'hands-off' crime, as there is no physical contact between the victim and the offender. This is a mistake, as abuse in front of the web cam does take place. The expression 'Live Distant-Child Abuse' seems to capture the nature of the crime more effectively. For the same reason the term 'Virtual Travelling Sex Offenders' appears to be inappropriate, as it minimises the role of the offender/viewer of the web cam sex performance in the process of abuse. Furthermore, the potential connection between pay-per-view abuse and Transnational Child Sex Offenders (TCSO), leading to hands on abuse, should not be neglected.

LE specialists report that in cases of LDCA the initial contact between a pay-per-view offender (customer) and a victim is often through a 'facilitator'. Contact occurs through a number of internet dating sites, internet chat sites as well as through offenders travelling to destination countries. Once contact is established, offenders and facilitators then utilise legitimate chat sites to communicate.

According to LE representatives in a number of DLCA cases, examination of the offender's computer devices or other electronic media storage devices often results in no electronic evidence of the child sex shows being identified. It is believed that these particular offenders are not downloading, recording or storing images and videos during the offending to purposefully avoid detection by LEAs. The low cost of pay-per-view child sex abuse makes it possible for offenders to view the abuse regularly without the need and risk of downloading it. The frequent small amounts of money being transferred minimise any red flags from financial transaction monitoring agencies[44].

A recently concluded operation led by the UK's National Crime Agency, the Australian Federal Police and US Immigration and Customs Enforcement in cooperation with the Philippines National Police, dismantled a paedophile ring that streamed live sexual abuse of children as young as six over the Internet. In some cases, the victims' parents were involved. 15 victims in the Philippines aged between 6 and 15 were rescued, 29 people were arrested, including 11 in the Philippines. 12 countries were involved in the arrest of individuals who had been paying for the live abuse of children. Over GBP 37,500 was identified as having been paid for the live

---

[44] Contribution by Australian Federal Police

With the financial support of the Prevention of and Fight against Crime Programme
European Commission –Directorate-General Home Affairs

abuse of children by the customer network[45]. Three other ongoing investigations have identified 733 suspects[46].

The Philippines is also mentioned by other stakeholders among the top countries in the world for online viewing of child sexual abuse. Reports from one NGO are that the amount of money that Filipino children earn from DLCA varies, depending on the length of the show, the number and ages of children involved and the sexual acts performed in the show. Most victims state they receive between PHP 500 and 2000 (between USD 11.50 and 46) per abuse session, but some victims reported that they did not receive any payment at all, either because the foreigner failed to keep his promise to transfer money, or because they allowed themselves to be subjected to the abuse in the hope that the foreigner would become his or her boyfriend. When the child is recruited for distant live child abuse by a middleman, he or she usually only receives around PHP 200 (USD 4.60). The money is transferred through Western Union or Cebuana Lhuillier, a local money-transfer agency[47].

The real-time monitoring of streamed CAM is legally and technically challenging, including extended features such as broadcasts protected by passwords and extra layers of anonymity.

It seems that both prioritising the identification of individuals who have access to children as well as developing a framework to identify suspicious financial transactions are, for the moment, the only methods of successfully combating this type of crime.

5. Commercial CSE – The Deep Web and the Darknet

Another example of the evolution of online commercial CSE comes from resources hosted in the Deep Web and the Darknet. Comparable crime data sets indicating an increase in the use of hidden services are very limited. However, there is evidence that the use of resources hosted in both environments by criminals dealing with distribution of CAM is evolving, including new forms of profit driven activity. It is important though to underline the distinction between the Deep Web and Darknet in this context. The Deep Web environment hosts online communities catering to those with a sexual interest in children and seems to be predominantly driven by financially motivated offenders and those engaging in online payment card fraud. The Darknet is mostly attributed to those dealing with distribution of CAM and other illicit markets.

---

[45] *http://www.nationalcrimeagency.gov.uk/news/news-listings/312-live-online-child-abuse-29-international-arrests-made*

[46] *http://www.naharnet.com/stories/en/114462-philippines-a-global-source-for-child-cybersex-industry*

[47] *http://terredeshommesnl.org/_media/documents/TdH-Fullscreen_on_View-Webversie_DEF.pdf*

5.1. Context - technological background

There is no doubt that hidden services have become more 'user friendly' in recent years, easier and quicker to use and therefore more attractive to less IT-savvy customers. Platforms like Tor and the hidden services therein, including 'Torchat', facilitate practically untraceable exchanges of images anonymously through websites, private messages and email[48].

The range of devices which can access the Darknet is also growing. Recent developments on Tor include the possibility of downloading Apps onto mobile Android devices, as well as 'safeplug' hardware to anonymise web browsing by linking to wireless routers and streaming data onto Tor[49].

The evolution of Bullet Proof Hosting services into Bullet Proof Clouds, provides not only web hosting but also comprehensive computing and back end processing that is entirely remote from the user's hardware. This still remains one of the most significant forensic challenges to the LE community, although according to them there is no evidence of the use of such resources for CSE related purposes yet.

If the process of duplicating communication services available on the Surface Web into the Darknet is going to continue, even live web streaming cannot be ruled out from the range of potential threats in the future. However unlikely this may seem today because of performance limitations, if there is a demand for such a service, technological constraints will be overcome in order to allow this.

LE representatives agree that Tor is the most popular platform, even after last summer's operation against Freedom Hosting[50]. No apparent loss of confidence in this network is noticeable, although various forums contain discussion threads on I2P distribution and also how to host content on Freenet. The impact on the CSE crime area of the recent Operation Onymous[51] law enforcement actions against other forms of criminality on the Darknet cannot be assessed at this stage.

5.2. Update on Commercial Distribution

The Darknet environment, providing anonymity to the publisher, viewer and server hosting material, is attractive to particular offenders, notably the ones with greater security awareness and technical knowledge. Peers inside those closed communities instruct each other, not only

---

[48] *iOCTA, P 30.*
[49] *Ibid., P 31.*
[50] *http://www.bbc.com/news/technology-23573048*
[51] *http://en.wikipedia.org/wiki/Operation_Onymous*

With the financial support of the Prevention of and Fight against Crime Programme
European Commission –Directorate-General Home Affairs

on 'How to practice child love'[52] but also providing detailed technical instructions such as the 'Information Security and Anti-forensics' guide[53].

Confidence in security and behavioural drivers may be the main reasons for differences between the Deep Web and the Darknet users with a sexual interest in children, casting the latter as an environment less profit oriented, where the highly desirable material tends to appear. Although this distinction is still valid, there is evidence that a demand for the new material is at the same time one of the crucial factors stimulating commercialisation in this environment.

As previously noted child abuse material itself holds a specific value. That value depends on its novelty; therefore it should not be a surprise that in some instances it may be an opportunity to profit. This opportunity may challenge the so far known characteristics of users of the Darknet as like-minded offenders, interested in posting and viewing CAM both securely and for free.

Instances when CAM is leaked from the Darknet to be sold on commercial websites on the Surface Web highlight the profit opportunities within this context. Again, the novelty of photos or videos will be a driving factor for such practice. The opposite situation may also take place, although the new material originating from the Surface Web is more likely to be used to upgrade a status rather than directly for commercial trade.

Users of the Darknet services interested in CAM have a general understanding that commercial dissemination violates their security, as some of the payment methods could be traceable, however it does not always prevent them from such activities. Since they are concerned with the anonymity and security of their performance, it is obvious that they will always be looking for payment methods offering them the same anonymity and security.

Discussions on Tor around raising money for CAM producers, including whether they would accept money and consumers would pay for it if they thought it was risk free, as well as asking users if they would be interested in producing material for gain, are the best evidence of the further commercialisation of this environment. Instances of bringing up dedicated sites for producers are not isolated anymore[54].

A real medium- to long-term consequence of this trend might be the situation where there are no limits - apart from a price range - to the kind of abuse a child could be subjected to if requested by a customer.

---

[52] *Document circulated in the Darknet.*
[53] *70-pages document circulated in the Darknet covering all aspects of security.*
[54] *http://www.deepdotweb.com/2014/11/09/as-drug-markets-are-seized-pedophiles-launch-a-crowdfunding-site/*

With the financial support of the Prevention of and Fight against Crime Programme
European Commission –Directorate-General Home Affairs

6. Developments in payment processes linked to commercial CSE online

While previous chapters of this assessment aimed at providing an overview of existing forms of commercial CSE online, this chapter focuses on the developments in the payment processes linked to them.

6.1. Reported payment methods

According to information provided by INHOPE, the following payment methods appeared in 5236 URLs suspected of the commercial distribution of CAM (registered in 2013):

- Money transfer services - 266
- Credit card payments - 135
- Digital wallet operators - 102

It is worth highlighting that, at the time of writing, the INHOPE database allowed the selection of some alternative payment options, and the technical implementation of further features and multiple payment options is already under discussion. Nevertheless, this limits the number of determined methods of payment in the data set.

Similar payment methods (ranked in order of frequency) have been reported by the IWF through both 2012 and 2013:

- Money transfer services
- Credit card payments
- SMS payments
- Digital wallet operators

It should be noted as a general trend that, even if major payment brands are offered, when the payment process is followed, the CAM content supplier seeks payment outside of the standard payment options.

On the LE side, specialists continue to report money transfer services and other alternative payment systems as the most prominent payment options for CAM.

6.1.1. Money transfer services

Money transfer services are the most cited by LE in relation to live web streaming. It is particularly difficult to estimate the extent of their misuse for the payment of CAM, as the pattern of the transactions are low value transactions (usually less than USD 100), from senders with no apparent family links to the receivers, going once or twice a week from developed countries, to those in South East Asia. In recent cases the majority of these payments were made on-line. However, this pattern is also common with other types of funding, including charity payments, which makes its detection even more difficult.

With the financial support of the Prevention of and Fight against Crime Programme
European Commission –Directorate-General Home Affairs

Money transfer services are also used to charge prepaid cards, which again ensure zero visibility on the nature of the transaction. A link of this method of payment to virtual currency has also been detected.

6.1.2. Credit card payments and digital wallet operators

A proactive approach by reputable companies, a number of regulations, compliance programmes and preventative work appear to have been effective in reducing the number of sites able to process payments. The downward trend in credit card payments previously observed by LE has been confirmed by information provided by EFC members, Visa and MasterCard.

Also, the use of digital wallet operators purporting to accept payment for CAM remains relatively low.

The situation described above can evidence a consensus that some mainstream payment methods have been eliminated from commercial CAM distribution online, although they are still being advertised on commercial child sexual abuse webpages. It does not mean however that this phenomenon has decreased because of this, but rather that it is evolving towards new digital environments.

6.2. Virtual currencies, anonymous online payment systems and underground markets

Although much of the evidence is still anecdotal, concerns have been expressed by LE and financial experts in the wider international environment that commercial CSE online, among other criminal activities, is moving to a new unregulated, unbanked digital economy[55]. Payment mechanisms providing a certain degree of anonymity are always open to abuse by those with criminal intentions, as developments in the use of Bitcoin show.

At the time of the last report, there was insufficient information to identify Bitcoin as a prominent payment method for CAM in the EU. One year later there is some evidence proving its attractiveness to CAM distributors and purchasers.

In January 2014, the IWF encountered the new payment mechanism in which Bitcoin is exclusively being accepted for the purchase of child sexual abuse images and videos on the Surface Web. Spam emails were used to distribute URLs to internet users. These URLs led to a hacked legitimate business website and would further re-direct the user to commercial child

[55] *For user concern on this, see https://www.hsdl.org/?view&did=747209, and testimony of Ernie Allen, ICMEC President and CEO, for the US Senate Committee on Homeland Security and Governmental Affairs.*

sexual abuse images on a second hacked website[56]. By July 2014, the IWF had identified 22 websites hacked with commercial templates exclusively accepting Bitcoin.

Bitcoin is also preferred by most of the Darknet vendors because no competitor has more liquidity, price stability, or widespread adoption. In terms of the Darknet adoption, the next closest currency is Litecoin, which historically averages about 5% of Bitcoin's market capitalisation[57].

But users of Darknet services are constantly looking for better ways to stay anonymous, which has led to new emerging crypto-currencies. Of those crypto-currencies with the potential to challenge Bitcoin's prevalence in the Darknet, Anoncoin was the first to release support for the Tor and I2P privacy networks, allowing users to hide their network identities from peers[58]. Another source mentions Darkcoin as the one which might act as an ultra-private counterpart to the foundational cryptocoin, and has enjoyed the most sustained community support[59].

Developers of technologies which promise truly anonymous and fast web transactions claim that Darkcoin is about providing privacy to protect users from government snooping, corporate involvement, and against criminals seeking to exploit payment information. They do however acknowledge that black market use may be an inevitable outcome of anonymity[60]. Obviously, the open question is still whether there will be further adoption of newly developed anonymous cryptocoins currencies by existing underground markets, although payment for CAM still seems to be rare there.

In autumn 2013, Silk Road, the infamous marketplace for illicit goods which had alleged web links to CAM concealed in the block chain of Bitcoin transactions, was taken down. This gap has been filled very fast, and according to open sources, Agora became the leader in the Darknet anonymous market activity, and bigger than the Silk Road ever was. The Silk Road 2.0, Evolution, Hydra and Middle Earth were also described as thriving[61] until some of them were taken down as a result of joint LE operations[62].

At the time of Operation Onymous, large amounts of existing underground markets (~33)[63] provided options for customers looking for illegal goods and services. The ongoing

---

56
http://www.theregister.co.uk/2014/03/03/iwf_says_hacking_and_bitcoin_trend_used_by_child_abuse_image_peddlers_is_possible_side_effect_to_uk_network_level_filtering/
https://www.iwf.org.uk/about-iwf/news/post/388-bitcoins-accepted-for-child-sexual-abuse-imagery
57 http://www.deepdotweb.com/2014/09/18/can-anoncoin-be-the-currency-of-the-deep-web/
58 Ibid.
59 http://www.deepdotweb.com/2014/10/21/darkcoin-bow-accepted-minor-dark-net-marketplaces/
60 http://www.ibtimes.co.uk/darkcoin-perfect-e-cash-cryptocurrency-emerging-dark-web-trump-bitcoin-1472144
61 http://www.idgconnect.com/abstract/8985/the-dark-net-will-black-market-continue-rise
62 Taken down on 06/11/2014; http://www.theguardian.com/technology/2014/nov/06/silk-road-20-owner-arrested-drugs-website-fbi
63 http://www.deepdotweb.com/2013/10/28/updated-llist-of-hidden-marketplaces-tor-i2p/

With the financial support of the Prevention of and Fight against Crime Programme
European Commission –Directorate-General Home Affairs

development of such payment availability in terms of commercial CAM distribution should be carefully monitored.

Greater enforcement attention should also be given to services like WebMoney or Perfect Money, including exchangers around them, as an alternative to former customers of Liberty Reserve (LR). The case of LR shows that regardless of the 'Know Your Customer' rules applied by this company, exchangers recommended on the website tended to be unlicensed money transmitting businesses operating without significant governmental oversight or regulation, concentrated in Malaysia, Russia, Nigeria and Vietnam[64].

The availability of the above mentioned resources, as well as the existence of many supportive ones enabling online money transfers to create perfect opportunities for successful, hardly traceable payments for commercial distribution of CAM and laundering of its profits, are among the biggest challenges for the LE environment.

6.3. Mobile Payment Systems

Information gathering on the misuse of mobile payment[65] systems in the commercial distribution of CAM was one of the recommendations of the previous assessment.

Numbers provided by INHOPE indicate only 3 reports requiring a payment through SMS in 2014[66], and 16 in 2013. The IWF data from 2013 confirms that mobile payment by SMS and paid call remains low, with only one recorded instance where a UK SMS shortcode was associated with live payments for CAM.

The research undertaken by the GSMA Mobile Alliance against Sexual Abuse Content corroborates the above, and informs that it is still rare for mobile payment mechanisms to be offered as an option on commercial CSE sites[67].

Furthermore, it reveals that commercial CAM websites offering premium SMS payments are typically limited to a small number of geographical regions, that the payments have separate short codes for each country and therefore are not working cross-border. Furthermore, a premium SMS is almost always seen as one payment option amongst a longer list including traditional payments services, such as credit and debit cards, stored value accounts (SVAs) and digital currencies.

---

[64] Lawrence Trautman, Virtual Currencies Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox, 20 RICH. J.L. & TECH. 13 (2014), http://jolt.richmond.edu/v20i4/article13.pdf.

[65] The term 'mobile payment' can be applied to any payment option which enables a payment to be carried out via mobile devices.

[66] Up to 25/05/2014.

[67] http://www.gsma.com/newsroom/preventing-mobile-payment-services-from-being-misused-to-monetise-child-sexual-abuse-content/

With the financial support of the Prevention of and Fight against Crime Programme
European Commission –Directorate-General Home Affairs

In comparison to other mainstream payment services, there is an extended time period for provisioning of services and deferred pay-outs. Operators are typically required to withhold pay-out on premium services for a minimum of 30 days to cover potential fines, versus weekly or daily pay-outs for the banking sector and 'instant' for stored value accounts. This makes mobile payment services naturally hostile to illicit businesses wishing to make quick money and a quick exit[68].

On being asked if any upcoming technologies in the mobile payment space might pose future threats, GSMA reported that there are a number of future developments in the mobile payment space generally, and digital commerce is one of four priority areas for the GSMA's Vision 2020 programme.

They offer the following examples:

- The B2B Wallet Interfaces programme seeks to create better interfaces with online (and retail) merchants;
- Mobile Money Interoperability has the following vision: 'Mobile money scales successfully as a digital payment solution, providing users with the same ubiquity of acceptance and simplicity as cash or card schemes. Interoperability between mobile money schemes gives a better customer experience & increases the addressable market size'[69].

Whilst these are not new technologies, and the programmes mentioned above have formal commitments to promote responsible business practices and work with the GSMA Fraud Forum to identify risks and associated controls, one could argue that increased growth in mobile commerce services may bring increased opportunities for abuse simply because of scale. Similarly, there are now examples of CAM distribution that is facilitated entirely by mobile connectively and it has recently been reported by LE that there are instances of mobile payments for online live abuse of children being re-directed to Africa. With this in mind, this area should be carefully monitored to identify any risks and associated controls in the near future. The GSMA Mobile Alliance has undertaken to formally seek updates from informed sources on an annual basis.

7. Emerging Issues & Future Considerations

In the previous report the consequences of Internet adoption in new regions, CAM distributors making use of online personal file storages as well as the next generation of hidden and bullet

---

[68] *Ibid.*
[69] *Contribution by GSMA.*

With the financial support of the Prevention of and Fight against Crime Programme
European Commission –Directorate-General Home Affairs

proof services, were mentioned as examples of potential future considerations, therefore attention should be given to some new future oriented threats.

As it has been rightly spotted by ICMEC 'there is apparent migration of commercial child sexual exploitation, along with other criminal enterprises, from the traditional payments system to a new, largely unregulated digital economy made up of hosting services, anonymising internet tools, and pseudonymous payment systems'[70].

More anonymity and encryption in online behaviour are undoubtedly among the most important future challenges. In particular, users will soon not require very sophisticated knowledge but just easily used and widely available hardware.

The further proliferation of underground markets, including the adoption of currency offering the highest anonymity, will continue. Development of fully peer-to-peer online marketplaces, posing particular difficulties for taking them down in case of any illegal activity, may create additional opportunities for CAM distribution[71].

Additionally, any changes in society that may facilitate crime should not be neglected. Sharing sexualised content online seems to be a part of adolescent development and of the sexual exploration processes of young people who nowadays have become members of a digital society by default. Materials originally produced for private consumption now end up in unwanted circulation and happen to attract the attention of people with a sexual interest in children, or profit oriented individuals who may use them as part of grooming or threatening processes.

Awareness campaigns should not be limited to minors only. Parents also need to be aware of the existence of social network profiles such as 'The most sexy 4, 5, 6 years old'. These profiles can access and use photos of people's offspring from their own profiles for less than innocent purposes. Such opportunism on the part of those operating those profiles emphatically proves that there is a great need to educate, not only children, but also their parents.

8. Legislative developments

The most interesting legislative developments are linked to the transposition of the Directive 2011/93/EU by Member States (apart from Denmark), which should have taken place by 18 December 2013.

---

[70] *ICMEC, The Digital Economy, P 11.*
[71] *http://www.wired.com/2014/08/openbazaar-not-for-drugs/*

At the time of writing, a review to evaluate the transposition into national law of the Directive is being conducted by Missing Children Europe, ECPAT and eNACSO with regard to seven topics, out of which three are the most relevant for the report:

- *Online grooming* (solicitation by means of information and communication technology of children for sexual purposes; Article 6 & Recital 19, topic 2 of the survey);
- *Extraterritorial jurisdiction* (Article 17 & Recital 29, topic 5);
- *Measures against websites containing or disseminating child pornography*[72] (Article 25 & Recitals 46 & 47, topic 7).

Although the final findings of the survey are not yet ready, preliminary results are available with respect to *Online grooming* (topic 2) and *Measures against websites containing or disseminating child pornography* (topic 7)[73].

The main problems identified to date are with regard to the transposition of Article 6(2). On the one hand the provision refers to online grooming of a child in order to obtain pornographic material depicting that child while, on the other hand, it refers to the online 'attempt' to commit the offences listed under Article 5(2) (acquisition or possession of child pornography) and 5(3) (knowingly obtaining access to child pornography). The result is that many reports do not really or clearly address the transposition of Article 6(2), while others consider that Article 6(2) is adequately transposed through general legislation on 'attempts' to commit specifically defined offences such as grooming. The result of all this is that at this stage of the study, in a majority of cases the transposition of Article 6(2) is unclear.

Regarding topic 7, from the point of view of access blocking as an additional protective measure, prior to the removal of the pages offering the CAM, the survey provides a positive result. A 2/3 majority of the MS reviews have indeed opted for some form of access blocking.

It should be noted that there are some other regulations which are relevant for this report and are not covered by the survey.

In Recital 16 of the Directive, Member States (MS) are invited to consider providing for the possibility of imposing financial penalties in addition to imprisonment, especially for those cases where the offences referred to in the Directive are committed with the purpose of financial gain. Moreover, in Article 11 of the operative part of the Directive, MS are encouraged to take the necessary measures to ensure that their competent authorities are entitled to seize any instrumentalities and proceeds from the offences referred to in Articles 2, 3 and 5 of the Directive. It would be very interesting to learn how these provisions are transposed to national

---

[72] *The term 'child pornography' is considered by specialists dealing with CSE as inappropriate. It is suggested to use the term 'child abuse material' instead.*
[73] *Contribution by Missing Children Europe.*

With the financial support of the Prevention of and Fight against Crime Programme
European Commission –Directorate-General Home Affairs

law especially in the context of successful prosecutions of EU citizens for the commercial distribution of CAM, which could serve as examples of good practice to be replicated throughout the European Union.

Among the latest developments influencing the area of research, the decision of the European Court of Justice on the Data Retention Directive, which mandates that telecom operators must retain all their customers' communications data for up to two years[74], should be highlighted. The court declared the Directive invalid, taking the view that it interferes, in a particularly serious way, with the fundamental right to respect for a private life and to the protection of personal data. Furthermore, when data is retained and subsequently used without the subscriber or registered user being informed, the persons concerned are likely to feel that their private lives are under constant surveillance[75] .

At the time of writing, data retention had been unanimously rejected by every supreme court and constitutional court to consider it being held unconstitutional in Austria, Bulgaria, Cyprus, the Czech Republic, Germany, Romania, and Slovenia[76], although there are examples of an opposite approach. The UK introduced a new data retention law in July 2014 in order to prevent UK ISPs from stopping to gather data on their users. Also in Sweden, with the backing of a Swedish administrative court ruling, the collection of user data to aid LE investigations is resuming.

It is of note that there are some legal developments outside of the EU, which are important examples of attempts to align the law with changing technology and online behaviour.

Authorities in Canada recently published a Bill with a maximum five-year prison sentence for anyone using the Internet to spread pornographic images of people they know. However, concerns have been expressed that the Bill could end up criminalising teenagers for 'idiotic mistakes' and potentially land them in prison. The Bill has also been criticised for giving legal immunity to telecommunications companies who voluntarily hand subscriber information to police and other public officials. As is the case with similar controversies in Britain, the Bill has been dubbed 'a snoopers' charter'[77].

In November 2014, authorities in the Australian state of Victoria introduced a ban according to which anyone who maliciously or deliberately spreads intimate images of another person - or

[74] *Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (OJ 2006 L 105, p. 54).*

[75] *Court of Justice of the European Union Press Release No 54/14 Luxembourg, 8/04/2014.*

[76] *http://www.digitalrights.ie/data-retention-slovenia-unconstitutional/*

[77] *http://www.independent.co.uk/incoming/new-canadian-revenge-porn-law-could-land-teenagers-in-prison-critics-argue-9593007.html*

With the financial support of the Prevention of and Fight against Crime Programme
European Commission –Directorate-General Home Affairs

threatens to do so - faces prosecution under two new offences. The ban applies to intimate images of anyone under the age of 18 as well as images of adults without their consent. The new law also introduce exceptions to child pornography offences, so those under 18 will not be prosecuted or placed on the sex offenders' register for consensual, non-exploitative sexting[78].

9. Concluding Remarks & Recommendations

A general recommendation is that the findings of this report should inform the activities of the other EFC Work Packages, and of the European Commission's EU/US Global Alliance against Child Sexual Abuse Online. More specific recommendations are as follows:

Cooperation

- Consensus on a pragmatic working definition of what can nowadays be assessed as commercial CAM distribution online should be worked out in cooperation between LE, hotlines, and the private sector.

- The new definition should to be incorporated in training sessions on commercial content assessment involving relevant actors, aiming for a more coordinated approach to the way hotlines assess commercial content, both in the way they collect relevant information and in the standardisation of this process.

- Raising awareness about new forms of criminal behaviour such as commercial sexual extortion.

CAM content related activities

- Further engagement in a campaign promoting technology that tracks the abuse-content itself, including the proactive identification and removal of CAM based on hash and photo DNA techniques. This should be accompanied by discussions on the standardisation of those tools, to avoid duplication of efforts in a process of exchanging and processing CAM related information.

- Further promotion of both prompt removals of web pages containing or disseminating CAM, as well as blocking access to them in overseas countries known for hosting them,

---

[78] *http://www.news.com.au/national/breaking-news/sexting-now-banned-in-victoria/story-e6frfku9-1227110428912?from=public_rss*

With the financial support of the Prevention of and Fight against Crime Programme
European Commission –Directorate-General Home Affairs

including newly connected regions. Through Work Package 4, the EFC should promote good practice in effective communication among LE, hotlines, and ISPs.

- A discussion should be initiated on a more proactive approach by file hosting and file sharing services in identifying and mitigating CAM, or regulations in this area could even be considered.

Payment mechanisms

- Data gathering from payment providers attached to the cyberlocker websites to gain knowledge of where the money is going and what payment methods are being used by the offenders. Implementation of best practices to prevent the on boarding of rogue cyberlocker merchants should be a minimum requirement by acquirers and agents when accepting contracts with merchants.

- Direct engagement with representatives of alternative payment systems to determine opportunities for better cooperation with LE, including common training for the better identification of payment processes linked to commercial distribution of CAM.

- Further exploration of commercial distribution business models in hidden services.

- Monitor the Deep Web and the Darknet criminal markets to determine proliferation of commercial CSE as a potential consequence of further migration from a traditional payment system to a new, largely unregulated digital economy.

Legislation

- In accordance with Recital 16 and Article 11 of the Directive 2001/93/EU, promote good practice amongst the judiciary in legislative interpretation of offences committed for financial gain.

With the financial support of the Prevention of and Fight against Crime Programme
European Commission –Directorate-General Home Affairs